REMARKS

Prosecution of the above-identified patent application has been reopened following the Notice of Appeal filed February 5, 2009 and the Appeal Brief filed April 6, 2009. However, claims 1-21 stand rejected in the Office Action dated September 18, 2009. For the following reasons, Applicants request reconsideration and withdrawal of the rejection.

Claims 1-4 and 12-16 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. App. Pub. No. 2002/0059286 (Challener) in view of U.S. Pat. App. Pub. No. 2003/0198350 (Foster). Applicants note that introduction to this rejection in section 1, on page 3 of the Office Action does not mention claims 8 and 20, but the rejection in section 6, on page 8 of the Office Action is also applied to claims 8 and 20. Applicants respectfully traverse the rejection of claims 1-4, 8, 12-16, and 20.

Challener is directed to trusted computing platforms, which in order to comply with Trusted Computing Platform Alliance (TCPA) standard must use 2048-bit RSA strings in a tree structure. Challener indicates that the 2048 bit lengths of the strings required by the TCPA standard make manipulations slow. See paragraphs [0003] and [0004] of Challener. Challener further teaches that use of a second tree structure that matches TCPA tree but contains keys of other types that require less time to manipulate, can improve performance of a trusted computing platform. Neither of the tree structures disclosed by Challener are related to consolidation of key updates.

Foster is directed to broadcast cryptography such as used in cable television systems. In such systems, a title key, which is needed to decrypt broadcast content, is recoverable from a key management block (KMB) that is transmitted with the content. Foster is particularly directed to reducing the size of the KMB, which can grow as the subscriptions of receiving devices are revoked. More specifically, Foster teaches revoking a KMB in the form of a logical key hierarchy corresponding to a first sub-tree of devices, and creating a smaller KMB for a second sub-tree of devices. See paragraph [0009] of Foster. Foster only maintains one tree structure at a time.

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

Independent claim 1 distinguishes over the combination of Challener and Foster at least by reciting, the "manager being arranged to store in association with each tree node, … the most up-to-date version of the encrypted key and its version information." Challener and Foster fail to suggest storing version information in association with each tree node. In the

rejection of claim 1, the Office Action on page 4 cites Foster and particularly paragraph [0045] of Foster. However, paragraph [0045] of Foster states, "a KMB typically includes a protected "version" of a key encrypting key as well as entries of revoked devices," and by that statement, Foster simply indicates that the title key is protected, e.g., encrypted. The protected version thus may correspond to an encrypted key, but Foster does not suggest use or storing version information, which is recited in claim 1 as being in addition to the encrypted key. Accordingly, the combination of Challener and Foster lacks any suggestion of storing the version information in the manner recited in claim 1.

In accordance with an aspect of Applicants' invention, a group member that may have missed one or more update records can use information from an apparatus of the type recited in claim 1 to construct up-to-date keys for secure communications within the group. The version information as described in Applicants' specification allows the group member to determine which keys in the group member's possession are up to date. Use of version information as recited in claim 1 would not be suggested by a combination of the systems of Challener and/or Foster because neither Challener nor Foster is concerned with up dating the key information of group members. In particular, Challener maintains an alternative key hierarchy to speed up key manipulations, and provides no indication that version information would be in any way useful. Foster does not update the key information of group member (or receiving devices) and storing version information is counter to the teaching of Foster because Foster seeks to reduce the size of a KMB,

For the above reasons, claim 1 is patentable over Challener and Foster.

Claims 2-4, 8, and 12 depend from claim 1 and are patentable over Challener and Foster for at least the same reasons that claim 1 is patentable over Challener and Foster.

Independent claim 13 distinguishes over the combination of Challener and Foster at least by reciting, "storing in association with each tree node, ... the most up-to-date version of the encrypted key and its version information." As noted above, the combination of Challener and Foster fails to disclose or suggest storing version information in association with each tree node. Accordingly, claim 13 is patentable over Challener and Foster.

Claims 14-16 and 20 depend from claim 13 and are patentable over Challener and Foster for at least the same reasons that claim 13 is patentable over Challener and Foster.

For the above reasons, Applicants request reconsideration and withdrawal of this rejection under 35 U.S.C. § 103.

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

Claims 5-7, 9-11, 17-19, and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over Challener in view of Foster and further in view of U.S. Pat. App. Pub. No. 2003/0126464 (McDaniel). Applicants respectfully traverse the rejection.

Claims 5-7 and 9-11 depend from claim 1 and are patentable over the combination of Challener and Foster for the reasons given above to show claim 1 is patentable. In particular, the combination of Challener and Foster do not suggest storage of version information and encrypted keys associated with nodes of a key hierarchy. McDaniel is directed to enforcing security policies and describes re-keying as one process that a security policy may require. However, McDaniel like Challener and Foster is not directed to and does not describe updating members of a group that have missed update records and also fails to suggest storing version information associated with nodes in a key hierarchy. Accordingly, the above reasoning showing claim 1 is patentable over Challener and Foster also applies to the combination of Challener, Foster, and McDaniel, and claim 1 and claims 5-7 and 9-11, which depend from claim 1, are patentable over the combination of Challener, Foster, and McDaniel.

Claims 17-19 and 21 depend from claim 13 and are similarly patentable over the combination of Challener, Foster, and McDaniel at least because claim 13 recites, "storing in association with each tree node, … the most up-to-date version of the encrypted key and its version information."

For the above reasons, Applicants request reconsideration and withdrawal of this rejection under 35 U.S.C. § 103.

For the above reasons, Applicants respectfully request allowance of the application including claims 1-21 as presented above. Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this document.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543